スノーデン暴露から10年を振返り、政府や警察による暗号弱体化の波を押し返す—グローバル暗号化デー参加イベント

小倉利丸
JCA-NET
2023/10/21

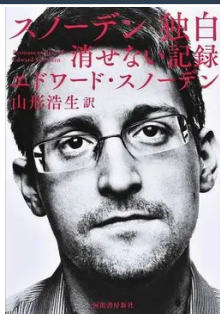
スノーデン暴露から 10 年 年表

- 2013 年、スノーデンは Đell と CIA での雇用を経て、 NSA の請負業者である Booz Allen Hamilton に雇用された。
- 自分が関与したプログラムに次第に幻滅するようになる。
- 2013 年 5 月 20 日、スノーデンはハワイの NSA 施設での仕事を終えて香港へ。
- 6 月上旬にジャーナリストの Glenn Greenwald 、 Laura Poitras 、 Barton Gellman 、 Ewen MacAskill に何千もの NSA の機密文書を暴露。
- この資料に基づいた記事がガーディアン紙、ワシントン・ポスト紙などに掲載され、国際的に注目されるようになる。

スノーデン暴露から10年 年表

- 2013年6月21日、アメリカ司法省はスノーデンに対し、スパイ活動法違反と政府財産の窃盗という2つの罪状で訴追を開始
- その後、国務省は彼のパスポートを失効させる。
- モスクワのシェレメーチエヴォ国際空港へ。彼は1ヶ月以上空港ターミナルに拘束。
- ロシアはスノーデンに亡命の権利を与える。
- 2020年10月、ロシアでの永住権を付与された。
- 2022年9月、スノーデンはロシア市民権を付与される。

出典：wikipedia 英語版

スノーデン関連の出版など

『スノーデン独白 消せない記録』山形浩生訳、河出書房新社、 2019

『スノーデン・ファイル徹底検証 日本はアメリカの世界監視システムにどう加担してきたか』 小笠原みどり、毎日新聞出版

『スノーデン監視大国日本を語る 』集英社新書 エドワード・スノーデン （著）, 国谷 裕子 （著）, ジョセフ・ケナタッチ （著）, スティーブン・シャピロ （著）, 井桁 大介 （著）, 出口 かおり （著）, 自由人権協会 （監修）、 2018

『監視社会をどうする！ 「スノーデン」後のいま考える、私たちの自由と社会の安全』日本弁護士連合会第６０回人権擁護大会シンポジウム第２分科会実行委員会 （編）、日本評論社、 2018

『スノーデンが語る「共謀罪」後の日本 大量監視社会に抗するために』岩波ブックレット、 スノーデン （述）, 軍司 泰史、 2017

『スノーデン日本への警告 』集英社新書、 エドワード・スノーデン、青木 理、井桁大介、金 昌浩、ベン・ワイズナー、マリコ・ヒロセ、宮下 紘、 2017

スノーデン関連の動画

OurPlanet-TV
あなたも監視されている〜スノーデンの暴露とは
小笠原みどりさんインタビュー
(2016)
https://yewtu.be/watch?v=A8sM_LafZqM&listen=false

OurPlanet-TV
デジタル監視と人権〜エドワード・スノーデン氏インタビュー
(2017)
https://yewtu.be/watch?v=AiAzPDm6vEM&listen=false

シテチズンフォー
松竹ホームビデオ (2017)
https://honto.jp/netstore/pd-dvd_87380388.html

JCA-NET

10月23日監視社会と暗号：グローバル暗号の日イベント
(2021)

https://vimeo.com/event/1337352/videos/618914958

スノーデン裁判

2020年9月
サンフランシスコの米連邦高等裁判所は２日、エドワード・スノーデン容疑者が暴露した米国家安全保障局（ＮＳＡ）による大量監視を違法とする判決を下した。大量監視を正当と主張していた米情報機関幹部は真実を語っていないと指摘した。

<u>連邦高裁は、何百万人もの米市民の通信記録を令状なく収集したことは外国情報監視法（ＦＩＳＡ）に違反している上、違憲の公算が大きいと言い渡した。</u>

スノーデン氏はツイッターへの投稿で、連邦高裁の判決はＮＳＡによる大量監視を暴露した自分の判断が正しかったことを裏付けていると強調。「裁判所がＮＳＡの活動を違法と非難し、判決の中で暴露した私の功績を認めたことを、生きているうちに見届けるなんて、想像すらしていなかった」と記した。（ロイター）

● スノーデンに対するスパイ活動法違反と政府財産の窃盗の罪について、ロイターの報道には言及がない。

スノーデンと大量監視

Brief discussion of global telecommunications infrastructure.

How access points in the US can collect on communications from "bad guy" countries (least cost routing, etc.)

左：ニューヨークタイムズが公開した国際通信ケーブルについての NSA の資料

右：EFF が裁判所に提出した大量監視の仕組みについての図

DOMESTIC INTERNET BACKBONE SURVEILLANCE

MILLIONS OF DOMESTIC INTERNET USERS

MILLIONS OF INTERNET USERS, WEBSITES, ETC

UNCONSTITUTIONAL SEIZURE

1 INTERCEPTION AND COPYING OF INTERNET BACKBONE COMMUNICATIONS STREAM

2 FILTERING AIMED AT EXCLUDING WHOLLY DOMESTIC COMMUNICATIONS

UNCONSTITUTIONAL SEARCH

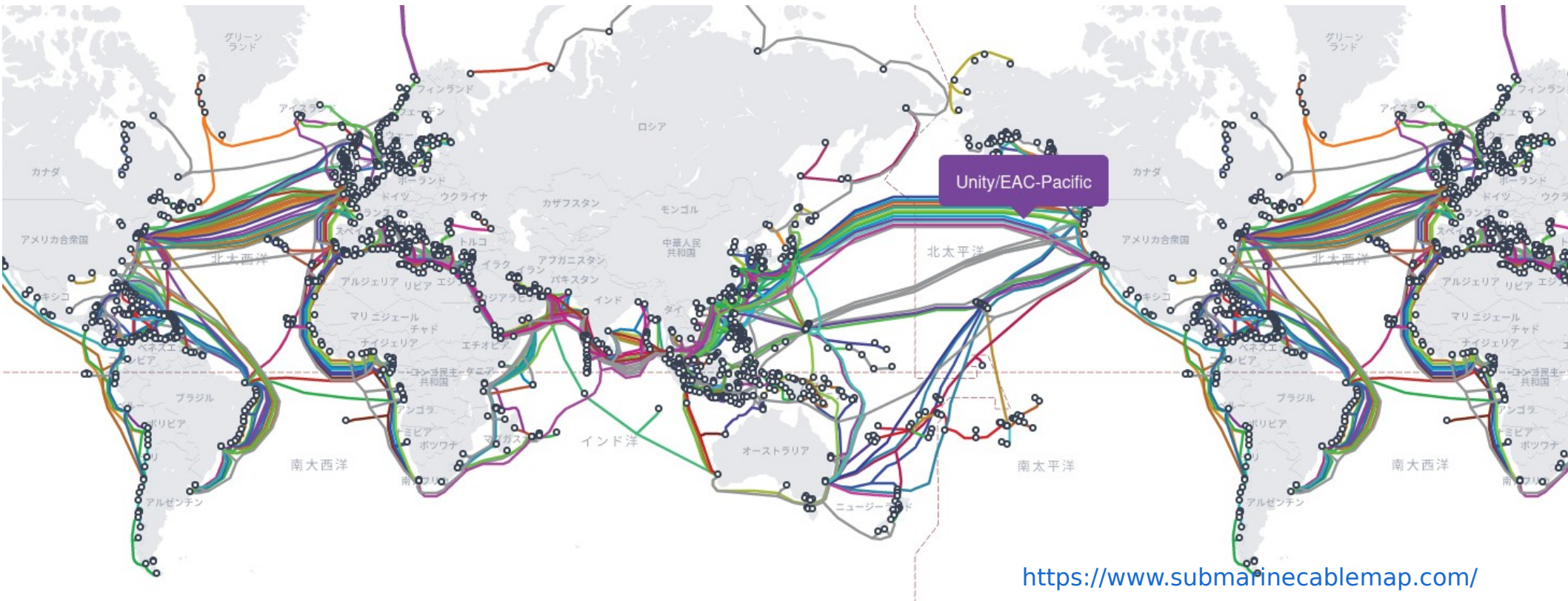
3 CONTENT SEARCHING OF FILTERED COMMUNICATIONS FOR SELECTORS

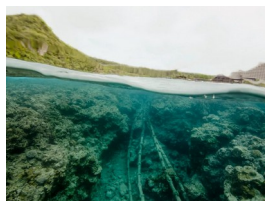
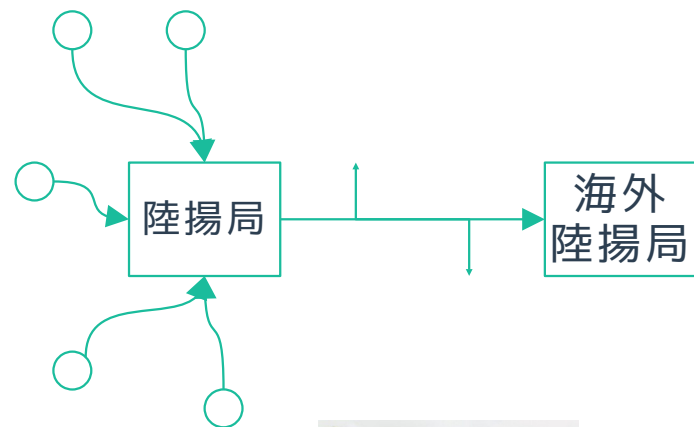
4 GOVERNMENT DATABASE OF COMMUNICATIONS CONTAINING A SELECTOR

GOVERNMENT SAYS A COMMUNICATION IS ONLY "COLLECTED" OR "ACQUIRED" IF IT CONTAINS A SELECTOR AND REACHES STAGE 4

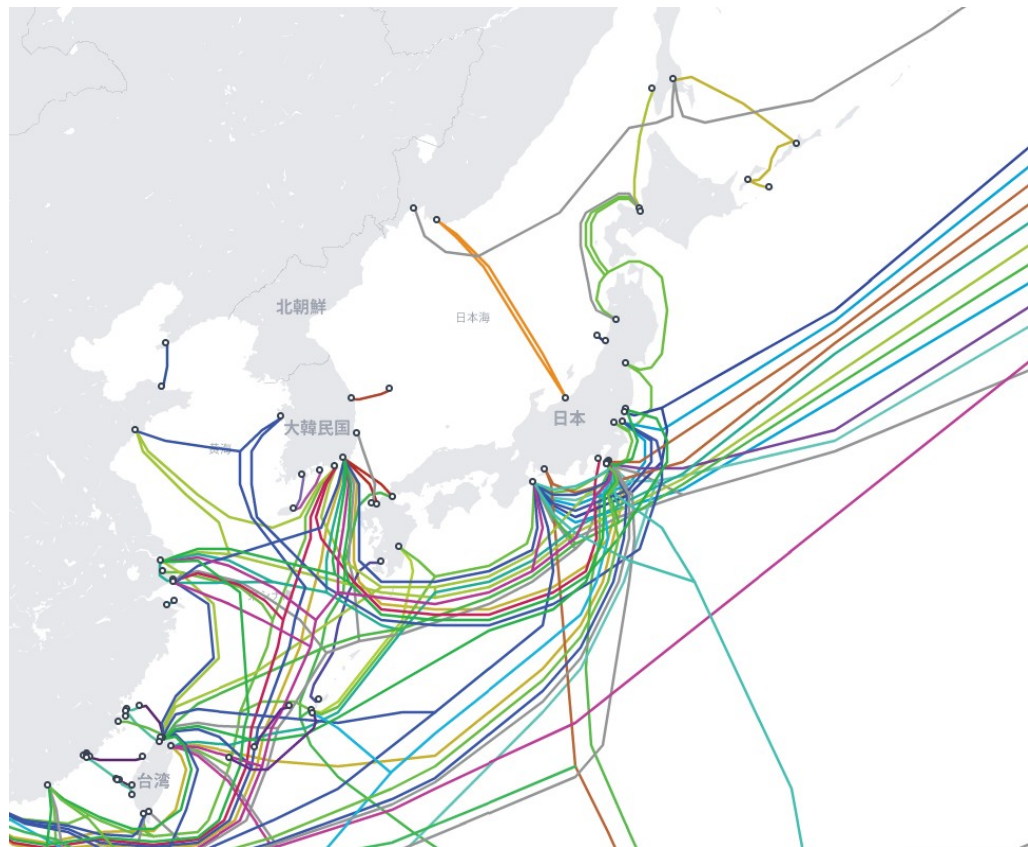
インターネットバックボーン（英：Internet backbone ）とは、インターネットの主要幹線を指す。商用、政府、学術、その他の大容量データ経路の相互接続された集合体であり、国家間、大陸間など世界中にデータを運ぶコアルーターの集合体である。（wikipedia）

スノーデンと大量監視

https://www.submarinecablemap.com/

スノーデンと大量監視

https://www.submarinecablemap.com/

写真家が捉えた、これが「NSAが監視する海底ケーブル」

北朝鮮
日本海
大韓民国
日本
台湾

データセンター、海底ケーブル等の地方分散によるデジタルインフラ強靱化事業 1

- 大規模震災の発生等が予測される我が国が、経済安全保障の観点等から、国内外のデータを「安全・安心」に蓄積・処理できるデータ・ハブとなるため、事業者が、東京圏以外※にデータセンター、海底ケーブル、インターネット接続点等のデジタルインフラを設置する際の支援を行い、地方分散による強靱な通信ネットワーク拠点を整備する。
- これらインフラ整備は、地方の課題を解決するためのデジタル実装を通じた地方活性化に資する。

※ 海底ケーブルは太平洋側以外

現状（東京圏一極集中のインフラ立地・太平洋側集中のネットワーク）

- **世界中でデータの急増する中、我が国のデータ・ハブ化の重要性**（**「経済安全保障」の観点**）
- **デジタルインフラが東京圏に一極集中する一方、高まる首都圏大震災の可能性**（**「国土強靱化」の観点**）
- **地方におけるデジタルの実装を通じた地方活性化**（**「デジタル田園都市国家」の観点**）

（インフラの立地状況　東京圏シェア）

（通信ネットワークの状況）

今後（DC、海底ケーブル、IXの地方分散を促進）

- **東京圏以外へのDC、海底ケーブル陸揚局、IXの設置**を支援し、**デジタルインフラの地方分散を促進**
- **太平洋側以外への海底ケーブル敷設**を支援し、**日本を周回する「デジタル田園都市スーパーハイウェイ」を完成**

令和3年度第1次補正予算：500.0億円（6カ年の基金） ※事業実施期間は令和3、4、5、6、7年度（5カ年） 令和8年度は出納整理年度

総務省
https://www.soumu.go.jp/main_content/000862736.pdf

スノーデンと大量監視

大きなプロバイダの多くは、アメリカのプロバイダと回線でつながり、インターネットの国際的（こくさいてき）な接続を行っています。これは、インターネットはもともとアメリカで始まったこともあり、世界各国のプロバイダがアメリカのプロバイダを中心にしておたがいにつながっているためです。プロバイダの中にはアメリカ以外にヨーロッパやアジアの国々のプロバイダともつながっているところもあります。各国とも、インターネット・エクスチェンジ（IX：アイエックス・Internet Exchange）を中心にして大きなプロバイダ同士がおたがいにつながっています。

全世界のインターネット接続を大きな視点（してん）で見ると、世界各国の大きなプロバイダがおたがいにつながるのと同時に、各国の国内でIXを通じておたがいにつながっています。これが、インターネットが世界のネットワークといわれる理由です。

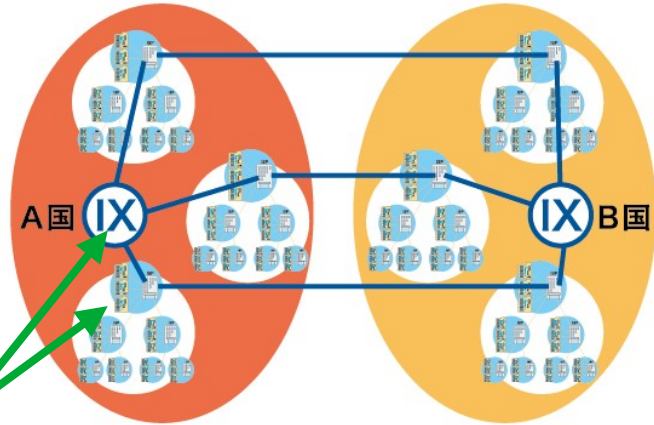
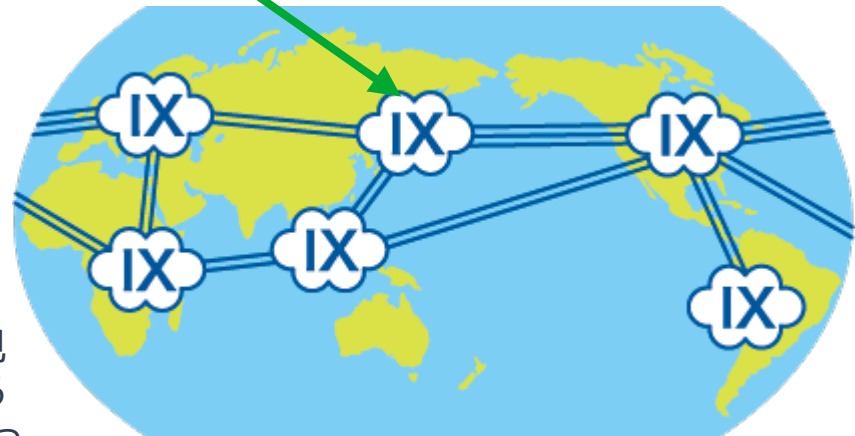



図5：プロバイダとプロバイダをつなぐインターネット・エクスチェンジ

総務省
https://www.soumu.go.jp/hakusho-kids/life/what/what_03.html

(RFC 9446) スノーデン暴露から 10 年を振り返る

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/rfc-9446_reflections-on-ten-years-past-the-snowden-revelations_jp/

今年はエドワード・スノーデンが米国の諜報機関などの膨大な機密文書を暴露して 10 年目になる。スノーデンが暴露した機密文書の内容は、米国をはじめとする諜報機関がインターネット以前からやってきた監視活動に危惧と関心をもってきた者にとっては、想定しうる事態であったとはいえ、実際に、その文書が生のまま示された衝撃はとても大きいものだった。 10 年という節目は、こうした大量監視を実際に遂行してる米国だけではなく、ほぼ全ての政府の情報機関などに対して、このスノーデンが自らの人生を賭けて行なった暴露がもたらした教訓を行かすことができるようになったか、私たちの監視されない権利がどれほど実現できてきたか、また、この権利のために私たちがどれほどの努力をしてきたのか、こうしたことを検証する機会になっていもいいだろう。以下は、主にインターネットの技術的な仕様の標準化に関わる技術コミュニティのメンバーなどが、この 10 年を振り返りながら、現状の問題を指摘したエッセイである。

(RFC 9446) スノーデン暴露から 10 年を振り返る

この文書は、インターネット技術タスクフォース（ IETF ）のなかにある技術文書 (RFC) のサイトに掲載されている。 IETF は一般にはなじみがないかもしれないが、「 IETF の使命は、インターネットをより良く機能させるような方法によって、人々がインターネットを設計、使用、管理する方法に影響を与える高品質で適切な技術的および工学的文書を作成すること」を使命として、インターネットを支える基本的な技術の標準化に関わる重要な活動を担っている。一般に RFC と呼ばれる文書の来歴はとても古く、インターネット草創期の 1969 年にまで遡る膨大な技術文書で、時系列に番号が振られている。ここに訳出したのは、その 9446 番目となる。ただし他の技術文書と違って、この文書には技術的な内容はなく、スノーデンが与えた衝撃を振り返りつつ、インターネットの技術コミュニティが抱えた課題を示す、ということが中心になっており、 RFC のなかでや特異だと思う。

(RFC 9446) スノーデン暴露から 10 年を振り返る

1. はじめに

2013 年 6 月 6 日、米国家安全保障局 (NSA) のある活動について記述した、スノーデン暴露とし て知られるようになった一連の記事の始まりとなる記事が、ガーディアン紙に掲載された [Guard2013]。これらの活動には、とりわけ秘密裁判所の命令、通信の発信元、宛先、タイミングを含むいわゆる「メタ情報」の受信に関する秘密協定、通信回線の盗聴が含まれていた。息をのむようなその活動範囲はインターネット技術コミュニティに衝撃を与え、IETF、IAB、その他の標準化団体に大きな変化をもたらした。

(RFC 9446) スノーデン暴露から10年を振り返る

2. Bruce Schneier：スノーデンの10年後

2013年9月に書いたものを再掲

ノーデンを取材したジャーナリストたちはコンピュータ・セキュリティの専門家ではない。専門家として彼等をサポートし、データの信憑性などを検証したのが、シュナイアーだった。

「私は8月下旬、グレン・グリーンウォルドの要請でリオデジャネイロに飛んだ。彼は数カ月前からエドワード・スノーデンのアーカイブに取り組んでいたが、より技術的な文書が山積みになっており、その解釈を手伝ってほしいとのことだった。グリーンウォルドによれば、スノーデンも私を射止めるのはいい考えだと思ったという。」

「私はグリーンウォルドが苦手としていた専門用語のいくつかを解読することができ、様々な文書の文脈と重要性を理解することができた。そして私は長い間、NSAの盗聴能力を公に批判してきた。私の知識と専門知識は、どの文書を報じるべきかを見極めるのに役立つはずだ。」

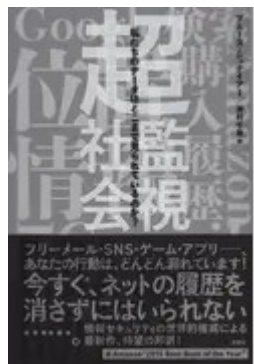
(RFC 9446) スノーデン暴露から 10 年を振り返る

『ハッキング思考 強者はいかにしてルールを歪めるのか、それを正すにはどうしたらいいのか』

日経ＢＰ 2023

『暗号技術大全』

ソフトバンクパブリッシング 2006

https://www.schneier.com/

『超監視社会 私たちのデータはどこまで見られているのか？』

草思社 2016

『暗号の秘密とウソ ネットワーク社会のデジタルセキュリティ』

翔泳社 2001

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier ：スノーデンの 10 年後

私が見たのは文書のごく一部で、そのほとんどは驚くほど平凡なものだった。トップシークレットの世界で懸念されるのは、システムのアップグレード、天候による運用上の問題、作業の滞りによる遅延など、主に戦術的なものだ。私は週報、状況説明会のスライド、訪問者を教育するための一般的なブリーフィングに目を通した。NSA の内部でも、管理職は管理職である。ドキュメントを読んでいると、果てしなく続く会議の一部を傍聴しているような気分になった。

会議のプレゼンターは、スパイスを加えようとしている。プレゼンテーションには、定期的に諜報活動の成功例が盛り込まれる。何がどのように発見され、どこで役に立ったかといった詳細があり、時にはそのインテリジェンスを利用した「顧客」からの賞賛もあった。これらは、NSA の職員に、自分たちが良いことをしていることを思い出させるためのものだろう。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier ：スノーデンの 10 年後

読んだものが特にエキサイティングだったわけでも、重要だったわけでもない。ただ驚かされたのだ。世界についての考え方が、ほんの少し変わった。

諜報の専門家は、内部で生活することがいかに方向感覚を失わせるかについて語る。世界の地政学的な出来事に関する機密情報を大量に読むと、世界の見方が変わってくる。ニュースメディアは間違っていることが多いので、何が本当に起こっているのかを知っているのは内部の人間だけだと確信するようになる。あなたの家族は無知だ。友人も無知だ。世界は無知だ。あなたを無知から守っているのは、絶え間なく流れてくる機密情報だけだ。優越感に浸らず、「私たちが知っていることをあなたが知っていれば」などといつも言わないようにするのは難しい。NSA の長官であるキース・アレグザンダー将軍が、なぜあれほど上から目線に見えるのか、私にはよくわかる。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier ：スノーデンの 10 年後

私はグリーンウォルドに、彼自身のオペレーション・セキュリティについて話をしようとした。ミランダが NSA の文書を USB メモリに入れて旅行していたのは、信じられないほど愚かなことだった。電子的にファイルを転送するのは暗号化のためだ。私はグリーンウォルドに、彼とローラ・ポイトラスはダミー文書の暗号化された大容量ファイルを毎日やり取りすべきだと言った。

...

私は自分のセキュリティ手順を疑い始めた。NSA のハッキング能力について読むと、そうなる。私のハードドライブの暗号は破れるのだろうか？おそらく無理だろう。私の暗号化ソフトを作っている会社は、その実装を意図的に弱めたのだろうか？おそらくそうだろう。NSA のエージェントは、私が米国に戻る通話を盗聴しているのか？おそらくそうだろう。諜報員がその気になれば、インターネット経由で私のコンピューターをコントロールできるだろうか？もちろんだ。結局、私は最善を尽くし、心配するのをやめることにした。結局のところ、それは所詮エージェンシーの書類だ。私が取り組んでいることは、数週間後には公になる。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier：スノーデンの 10 年後

私もよく眠れなかった。その理由の多くは、私が目にしたもののあまりの大きさだった。別に驚くようなことではなかった。<u>私たち情報セキュリティ関係者は、NSA がこのようなことをしていると長い間思っていた。しかし、実際に腰を据えて詳細を把握することはなかった。詳細を確認できたことは大きな違いだった。</u>

NSA が世界を盗聴しているのは間違いのない事実であり、しかもそのような計画的で強固なやり方で行っている、このことを知っているのと、それが現実であり、どのように行っているのかの詳細に直面するのとでは、まったく違う。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier：スノーデンの 10 年後

スノーデンはアメリカにダメージを与えたいのだ、という話を聞いたことがある。私は、彼はそうではないと断言できる。今のところ、この事件に関わった誰もが、公開する内容について信じられないほど慎重になっている。アメリカにとって計り知れないほど有害な文書がたくさんあるが、誰もそれを公開するつもりはない。記者たちが公開する文書は慎重に編集されている。グリーンウォルドと私は、『ガーディアン』紙の編集者と記事のアイデアのニュースバリューについて何度も議論し、単に面白いからという理由で政府の秘密を暴露することはないと強調した。

(RFC 9446) スノーデン暴露から10年を振り返る

2. Bruce Schneier：スノーデンの10年後

NSAから見れば、私を含め、私たち全員が重大なセキュリティ・リスクなのだ。私は機密事項に関するメモを取り、それをくしゃくしゃにしてゴミ箱に捨てていた。ホテルのロビーで“TOP SECRET/COMINT/NOFORN“と書かれた書類を印刷していた。そして一度だけ、間違ったUSBメモリを夕食に持って行き、誤って最高機密文書が入った暗号化されていない方のUSBメモリをホテルの部屋に置き忘れたことがある。どちらも青色だったのだ。 もし私がNSAの職員だったら、それだけで解雇されるだろう。

…

常に監視されていることがいかに人を変えるかについては、多くの人が書いている。監視されていることがわかると、自分を検閲するようになる。オープンでなくなり、自発的でなくなる。コンピューターに書き込んだことを見たり、電話で話したことをくよくよ考えたり、文脈を無視してどう聞こえるだろうかと、仮定の観察者の視点から考えたりする。より順応しやすくなる。自分の個性を抑えてしまう。何十年もプライバシーの仕事をしてきて、NSAとその仕事についてはすでによく知っていたにもかかわらず、その変化は手に取るようにわかった。その感覚は今でも薄れていない。私は今、自分の発言や書き込みにより注意深くなった。通信技術に対する信頼が薄れた。コンピューター業界への信頼も薄れている。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier：スノーデンの 10 年後

NSA の政府権限は何ら制限されていないのだ。そして、監視資本主義は依然としてインターネットのビジネスモデルである。

(RFC 9446) スノーデン暴露から 10 年を振り返る

2. Bruce Schneier ：スノーデンの 10 年後

2016 年に一度、モスクワに彼を訪ねた。そして数年間、ハーバード大学の私のクラスで、 Jitsi の遠隔操作で彼にゲスト講義をしてもらった。その後、私はセッションを開き、彼が言い逃れたり答えなかったりするあらゆる質問に答え、彼が答えたすべての回答を説明し、未解決の逮捕状が出されている人間にはできないような方法で率直に話すことを約束した。

…

しかし、もう 10 年も経っている。<u>彼が知っていることは、すべて古く、時代遅れだ。私たちが知っていることは全て古くて時代遅れになった。</u> NSA は 2016 年と 2017 年に、 Shadow Brokers を装ったロシアによる、さらにひどい機密漏洩に見舞われた。しかし NSA は立ち直った。 NSA は再び、私たちが推測することしかできないような能力を持つようになっている。

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

2013 年、 IETF 、そしてより広くインターネットの技術、セキュリティ、プライバシーの研究コミュニティは、スノーデンの暴露によって明らかになった監視と攻撃の取り組みに驚愕した [Timeline]。そのような可能性があることは知られていたが、非常に多くのインターネットエンジニアにとって憂慮すべきものであり、非常に厄介なものであったと言って差し支えないと思うのは、公開された活動の規模と広さであった。

…

IETF の反応としては、 2013 年 7 月にベルリンで開催された IETF 会議における非公式な会合で、 IETF の参加者は、これらの暴露は、 IETF プロトコルのセキュリティとプライバシーの特性を改善し、すでに存在するセキュリティとプライバシーのメカニズムをより確実に利用できるようにするために、私たちがもっと努力する必要があることを示していると考えていることが示された。

以後、攻撃に対する「インターネットの堅牢化」に関する活発が行なわれる

(RFC 9446) スノーデン暴露から 10 年を振り返る

(補足)

IETF とは。*https://www.ietf.org/*

The Internet Engineering Task Force (IETF) インターネット技術タスクフォース

「1986 年に設立されたインターネット技術タスクフォース(IETF)は、インターネットの主要な標準化団体(SDO)である。」

IETF のミッション・ステートメント

「IETF の全体的な目標は、インターネットをより良く機能させることである。

IETF の使命は、インターネットをより良く機能させるために、人々がインターネットを設計し、使用し、管理する方法に影響を与える、高品質で適切な技術的および工学的文書を作成することである。これらの文書には、プロトコル標準、現在のベストプラクティス、様々な種類の情報文書が含まれる。」

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

2014 年 2 月から 3 月にかけて、ロンドンで「広範な監視に対するインターネットの強化」[STRINT] に関する IAB/W3C 合同ワークショップが開催され、 150 人のエンジニアが参加

ラフ・コンセンサスが得られた重要な声明

" 広汎な監視は技術的な攻撃であり、 IETF プロトコルの設計において可能な限り緩和されるべきである。 *" (RFC 7258)*

この文書はその後、セキュリティとプライバシーに関する追加作業を正当化するものとして、多くの IETF ワーキンググループと RFC によって参照されている [Refs-to-7258] 。その期間とそれ以降も、スノーデンの暴露の影響は、 IETF の主要な技術管理組織である IAB と IESG (私は当時その委員を務めていた) の両方にとって、主要かつ継続的な議題であり続けた。

(RFC 9446) スノーデン暴露から 10 年を振り返る

(補足)

IAB(Internet Architecture Board)

IAB は、インターネットの技術コミュニティ全体の方向性やインターネット全体のアーキテクチャについての議論を行う技術者の集団です。ISOC の技術理事会(Technical Advisory Group)としても機能し、インターネットを支える多くの重要な活動を監督。

具体的には、IETF チェアと IESG メンバー等の任命や、インターネット技術およびアーキテクチャに関して ISOC への技術的アドバイスを行ったり、また、ITU-T、W3C、ISO など外部組織とのリエゾンについての最終的な責任も負う。

IAB の運営ポリシーならびに運営方法は、RFC2850 に記述されています。IAB は、12 名で構成され、各メンバーの任期は 2 年(再任可能)となっており、毎年 6 名ずつが改選されることになっている。

(https://www.nic.ad.jp/ja/basics/terms/iab.html)

(RFC 9446) スノーデン暴露から 10 年を振り返る

(補足)

IESG

「 Internet Engineering Steering Group 」の略。 IESG は IETF の活動と標準化プロセスの、技術的な側面についての責任を担っているグループです。 IESG のメンバーは、 IETF の複数の Working Group で文書のレビューを行ったり、 WG の方向性について助言を行っている Area Đirector で構成されています。

IESG は ISOC の理事によって批准された規則に従い、 RFC の草案にあたる Internet-Đraft の標準化プロセスを進めるかどうかを決定します。 Internet-Đraft は、 IESG によって承認されると RFC 番号が割り振られ、 RFC として IETF のサーバで公開されます。 https://www.nic.ad.jp/ja/basics/terms/iesg.html

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

IETF の参加者が少なくとも部分的にはスノーデンの暴露を動機として開始した技術的作業

「 2013 年 11 月、アプリケーションで TLS[Transport Layer Security] を使用するためのより良いプラクティスを文書化するためのワーキンググループが設立され [UTA]、 TLS のストリッピングや TLS API やパラメータの誤用に関連するいくつかの攻撃に直面しても、デプロイメントがより危険にさらされないようにした。同様の作業は、後に CURDLE Working Group [CURDLE] で、他のプロトコルにおける暗号の使用を推奨する勧告を更新するために行われた。 CURDLE Working Group は、 IRTF Crypto Forum Research Group [CFRG] によって文書化された新たな楕円曲線のセットを使用可能にするために設立された。この作業は、 NIST の乱数生成器が NSA の攻撃に対して脆弱な出力を生成するように故意に設計された DUAL_EC_DRBG の大失敗 [Dual-EC] (後述) の後、 NIST 標準で定義された楕円曲線に対する (おそらく最終的には根拠のない) 懸念が動機の一部となっていた。」

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

(参考)

2020-10-14 Đual_EC_ĐRBG のバックドアの仕組み

https://techmedia-think.hatenablog.com/entry/2020/10/14/235117

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell ： IETF とインターネット技術コミュニティの反応

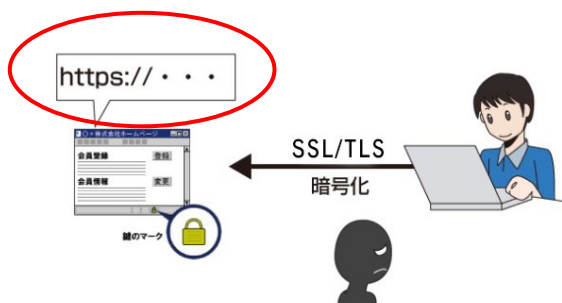
「 *TLS 1.2 およびそれ以前のバージョンの実装が、長年にわたってさまざまな攻撃に対して脆弱であることが示されてきたことを懸念して、 TLS の新バージョンを開発する作業が 2014 年に開始された。 TLS 1.3[RFC8446] を開発するための作業は、ネットワークの観測者により少ない情報を公開するように、ハンドシェイクの多くを暗号化することも目的としていた。<u>これは、スノーデンの暴露のかなり直接的な結果である。</u>この点で TLS をさらに改善する作業は、現在の TLS に存在する最後のプライバシー・リークの 1 つを取り除くために、いわゆる Encrypted Client Hello （ ECH ）メカニズム [TLS-ECH] を用いて今日も続けられている。*」

(RFC 9446) スノーデン暴露から 10 年を振り返る

(補足)

TLS とは

SSL (Secure Socket Layer) / TLS (Transport Layer Security) とは、インターネット上でデータを暗号化して送受信する仕組みのひとつです。クレジットカード番号や、一般に秘匿すべきとされる個人に関する情報を取り扱う Web サイトで、これらの情報が盗み取られるのを防止するため、広く利用されています。また、 SSL/ TLS は暗号化に加え、電子証明書により通信相手の本人性を証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_structure_13.html

(RFC 9446) スノーデン暴露から10年を振り返る

(補足)

TLSとは

TLSが提供するセキュアなチャンネルでは、

- 通信データを暗号化することで盗聴しても内容が分からないようにする
- 通信データが伝送される途中で改ざんされた時にそれを検出する
- 通信相手が正しいということを確認できる

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell ： IETF とインターネット技術コミュニティの反応

「 *ECH の取り組みは、 DNS over TLS （ DoT ） [RFC7858] または DNS Queries over HTTPS （ DoH ） [RFC8484] を使用して DNS トラフィックを暗号化する重要な開発によって可能になった。それ以前は、 DNS データや（より重要な） DNS データにアクセスする行為に関して、プライバシーはあまり考慮されていなかった。 DNS トラフィックを暗号化する動きは、インターネットにとって重要な変化を意味する。それは、平文を減らすという点でも、コントロールのポイントを移動させるという点でも同様である。後者の側面は議論の的であったし、今もそうであるが、 IETF はより良い DNS プライバシーを可能にする新しいプロトコルを定義するという仕事をした。 HTTP バージョン 2[RFC9113] と QUIC[RFC9000] に関する取り組みは、少なくともトランスポートレイヤー以上では、常に暗号化プロトコルを新しい標準とする IETF の流れをさらに示している。*」

(RFC 9446) スノーデン暴露から 10 年を振り返る

(補足)

ÐNS 暗号化について

https://blog.cloudflare.com/ja-jp/dns-encryption-explained-ja-jp/

「ドメインネームシステム(ÐNS)はインターネットのアドレス帳に相当します。cloudflare.com、あるいはその他のサイトにアクセスする際、ブラウザーは ÐNS リゾルバーに対しそのウェブサイトの IP アドレスを要求します。この時の ÐNS クエリと応答は残念なことに通常無防備です。ÐNS を暗号化することにより、ユーザーのプライバシーとセキュリティは向上します。この記事では、ÐNS を暗号化する 2 種類の方式、つまり ÐNS over TLS (ÐoT) および ÐNS over HTTPS (ÐoH) について説明します。また、その仕組みについても説明します。」

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

「 2013 年、 HTTPS は比較的使いやすかったにもかかわらず、ウェブはほとんど暗号化されていなかった。 ...

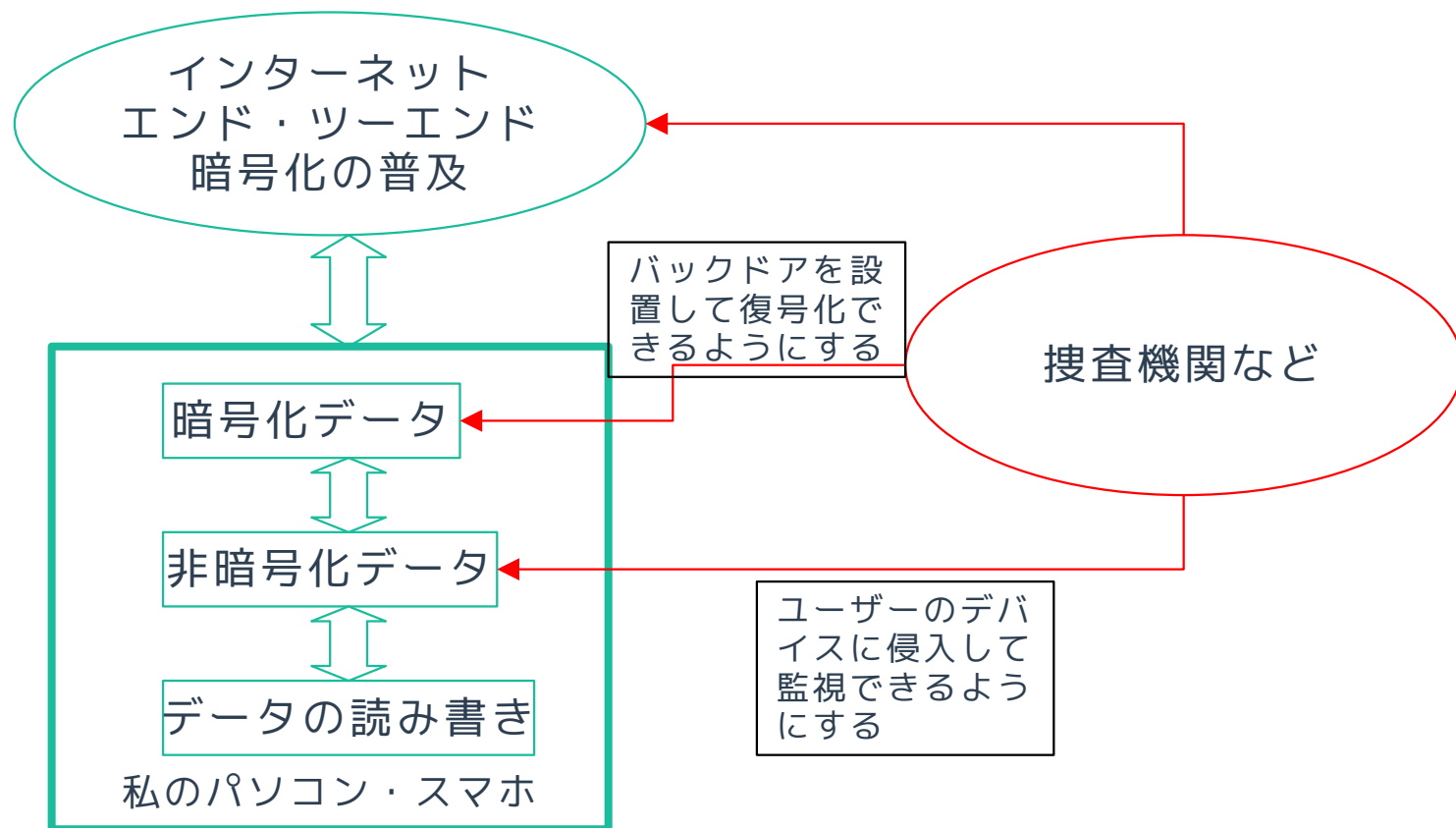
2013 年、メールサーバー間のほとんどのメール転送は平文であり、スノーデン文書に記された攻撃のいくつかを直接可能にしていた。その後、主要なメールサービスと MTA ソフトウェア開発者による多大な努力により、メールサーバー間で 90% 以上のメールが暗号化されるようになり、その状況を改善するために、 SMTP MTA Strict Transport Security (MTA-STS) [RFC8461] など、さまざまな IETF プロトコルが定義されている。

最後に、 MAC アドレスは歴史的にローカルネットワーク (およびそれ以 外) から見える長期的な固定値であり、スノーデン文書 [Toronto] で記録されたいくつかの トラッキング攻撃を可能にしていた。実装者、ベンダー、および IEEE 802 標準化グループは、この弱点を認識し、 MAC アドレスのランダム化に関する作業を開始し、その結果、 IETF の MAĐINAS ワーキンググループ [MAĐINAS] につながった。」

(RFC 9446) スノーデン暴露から 10 年を振り返る

3. Stephen Farrell : IETF とインターネット技術コミュニティの反応

「要約すると、スノーデンの暴露の結果、 IETF やその他の場所で追求された非常に大量の技術的な作業は、主に 2 つのことに集中している。1 つは、ネットワーク上の観察者から見えるプレーンテキストの量を減らすこと、もう 1 つは、デバイスやユーザの予期せぬ識別や再識別を可能にする長期的な識別子の数を減らすことである。この作業は決して完全ではないし、すべてに配備されているわけでもないが、大きな進展があり、攻撃に対する悩みの種は時間の経過とともにいくらか薄れてきたとはいえ、作業は続けられている。」

現在の問題：暗号化を弱体化＋暗号化を回避する政策との闘い

現在の問題：暗号化を弱体化 + 暗号化を回避する政策との闘い

日本政府は、2020年10月11日に発出された「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」（以下「ステートメント」と呼ぶ）に、英国、米国、オーストラリア、ニュージーランド、カナダ、インドとともに署名

外務省：https://www.mofa.go.jp/mofaj/la_c/sa/co/page22_003432.html

（１）システム設計に公共の安全を取り入れることにより、企業が違法なコンテンツや活動に対し、安全性を損なうことなく効果的に行動できるようにしつつ、違法行為の捜査や訴追を円滑化し、脆弱な人々を保護することができるようにすること。

（２）令状等が合法的に発行され、必要かつ衡平であり、厳格な手続と審査に服している場合に、法執行機関が読取可能かつ利用可能な形式のコンテンツにアクセスできるようにすること。

現在の問題：暗号化を弱体化＋暗号化を回避する政策との闘い

声明への批判

JCA-NET 理事会声明

暗号規制に反対します―日本政府は「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」から撤退を！！ https://www.jca.apc.org/jca-net/ja/node/105

国際共同声明：CDT、GPD、インターネット・ソサイエティは、時代遅れの暗号化バックドアの主張を認めない
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/cdt-gpd-and-internet-society-reject-time-worn-argument-for-encryption-backdoors/

現在の問題：暗号化を弱体化+暗号化を回避する政策との闘い

反対声明の骨子

(1)　憲法21条で定められた「通信の秘密」条項に明確に違反します。

(2)　法執行機関などが読取・利用できるように暗号化を弱体化させる技術の導入をIT業界に要求することに反対。

(3)　暗号規制は人権活動家、ジャーナリストなどによる広範な支援や当事者のプライバシーや「脆弱な人びと」をより脆弱にしてしまう。

(4) 法執行機関が私たちの通信の秘密に対して特権的な権限を行使できるような通信インフラを構築し、監視国家化を促すもの。

現在の問題：暗号化を弱体化 + 暗号化を回避する政策との闘い

最近の傾向

サービスプロバイダーに、コンテンツに違法性がないかどうかのチェックを義務づける法案が米国などで出されている。2023年インタラクティブ・テクノロジーの濫用・蔓延する不履行を排除する法律 the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 20233 (EARN IT, S.TK)

エンド・ツー・エンド暗号化では、プロバイダーは通信の内容を把握できない。この暗号化を弱体化させてプロバイダーがコンテンツを監視・検閲できるようにする。

現在の問題：暗号化を弱体化 + 暗号化を回避する政策との闘い

最近の傾向

英国のオンラインセーフティ法 (2023)

英国の規制当局であるOfcomに、エンドツーエンド暗号化によって提供されるセキュリティとプライバシーを損なうテクノロジーを使用し、コンテンツをスキャンすることによって大規模な監視を行うことをプラットフォームに強制する権限を与える

現在の問題：暗号化を弱体化＋暗号化を回避する政策との闘い

最近の傾向

EU チャット・コントロール、CSA規則

すべてのプライベートなチャット、メッセージ、電子メールを自動的に検索し、疑わしい内容がないかどうか、一般的かつ無差別に検索することをプロバイダーに義務づけようとしている。その目的は、児童ポルノを起訴することである。結果としては その結果、完全に自動化されたリアルタイムのメッセージングとチャットコントロールによる大量の監視と、デジタル通信の機密性の廃止が行われることになる。（Patrick Breyer）

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eu_messaging-and-chat-control_jp/

現在の問題：暗号化を弱体化＋暗号化を回避する政策との闘い

暗号規制の法制化などで実際にどのような影響がでるのか。

- エンド・ツー・エンド暗号化のサービスを利用すること自体が違法化される可能性がある。 Protonmail や Tutanota などの暗号化メールサービス、 Signal などの暗号化 SNS などが使えなくなる可能性がある。
- プロバイダーがユーザーのプライバシーを優先させて暗号化サービスを導入することが困難になる。
- プロバイダーが、捜査機関などの「手先」になってユーザーの通信内容を監視するようになる。

現在の問題：暗号化を弱体化 + 暗号化を回避する政策との闘い

この 10 年の意味

- スノーデン以後急速に普及してきた暗号化された通信によって、政府が言論・表現空間に対して有していた監視力の低下が顕著になる。これに対して、暗号化を規制し、政府の監視力の復権を図ろうとしている。
- 暗号規制の口実として各国が共通して用いているのが、子どもの性的搾取対策である。
- 暗号化をめぐる闘いは、現在非常に深刻になっている。米国、英国、EU が次々に具体的な法整備に着手しており、日本もこの傾向に向うことは必至といえる。

暗号化は私たちの言論表現の
自由を守る最後の砦です。
この砦が今危機にあります。